IFW

Attorney Docket No.: BHT-3092-413

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	:	
Sheng Shun YEN	:	Group Art Unit: 2131
Application No.: 10/760,392	:	Examiner: Not Yet Assigned
Filed: January 21, 2004	:	

For: **LOW PROFILE OF SECURITY USB DIGITAL DATA PROCESSING DEVICE**

CLAIM TO PRIORITY UNDER 35 U.S.C. § 119

Assistant Commissioner of Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Pursuant to the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55, Applicant claims the right of priority based upon **Chinese Patent Application No. 2003101244221 filed December 24, 2003.**

A certified copy of Applicant's priority document is submitted herewith.

Respectfully submitted,

By: _____
Bruce H. Troxell
Reg. No. 26,592

TROXELL LAW OFFICE PLLC
5205 Leesburg Pike, Suite 1404
Falls Church, Virginia 22041
Telephone: (703) 575-2711
Telefax: (703) 575-2707

Date: June 29, 2004

证　　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2003.12.24

申　请　号：　2003101244221

申请类别：　发明

发明创造名称：　一种对资料加密保护的USB界面资料处理卡

申　请　人：　劲永国际股份有限公司

发明人或设计人：　严圣舜

中华人民共和国
国家知识产权局局长　王景川

2004 年 2 月 9 日

权 利 要 求 书

1、一种对资料加密保护的 USB 界面资料处理卡，其特征为：至少具有一 USB 界面讯号，提供作为资料传输的方式；并具一 USB 界面控制器及一储存器单元，该界面控制器是处理界面资料后写入于该储存器单元，或处理该储存器单元内的资料后传输至界面上；同时具有一运算单元，其是提供上述 USB 界面控制器的运算能力，以提供资料加密保护的功能。

2、根据权利要求 1 所述的对资料加密保护的 USB 界面资料处理卡，其特征为：其中储存器单元是由至少一储存器所组成。

3、根据权利要求 1 所述的对资料加密保护的 USB 界面资料处理卡，其特征为：其中 USB 界面控制器与运算单元是整合于一半导体晶片。

4、根据权利要求 1 所述的对资料加密保护的 USB 界面资料处理卡，其特征为：其中 USB 界面控制器与储存器单元是整合于一半导体晶片。

6、根据权利要求 1 所述的对资料加密保护的 USB 界面资料处理卡，其特征为：其中进一步包括有一乱码产生器，以作为产生资料加密处理所需的参数。

7、根据权利要求 1 所述的对资料加密保护的 USB 界面资料处理卡，其特征为：其中运算单元是可提供 DES、TDES、RC2、RC4、RC5、RSA、DSA、SHA/SHA-1、MD2 或 MD5 演算能力。

8、根据权利要求 1 所述的对资料加密保护的 USB 界面资料处理卡，其特征为：其中储存器单元进一步区分成数个区段，其中包括有一保护区段，使用者无法在此区段内部进行对资料的读取，写入、删除、修改及格式化动作。

9、根据权利要求 8 所述的对资料加密保护的 USB 界面资料处理卡，其特征为：其中进一步利用适当的程序提供，可使特定的使用者对该保护区段内部进行对资料的读取、写入、删除、修改或格式化动作。

10、根据权利要求 1 所述的对资料加密保护的 USB 界面资料处理卡，其特征为：其中该资料处理卡是使用智慧棒的结构设计。

IN033772

说　　明　　书

—种对资料加密保护的USB界面资料处理卡

技术领域

本发明涉及为利用普遍使用的 USB 界面技术及一智慧棒(Intelligent Stick)的结构，建立起具有智慧卡(Smart Card)资料安全等级的资料安全系统，尤其涉及一种对资料加密保护的 USB 界面资料处理卡。

背景技术

目前广泛使用于金融服务的储存卡或认证卡，多是为智慧卡(Smart Card)系统所构成，然而其系统架设成本过高，且于个人电脑系统周边的支援上并不普及，因此有所谓 USB 的界面安全认证装置，以改善其缺点，但是其体积厚度又大于一般的储存卡，不易为使用者所便于携带。

因此，对于作为数位资料处理设备而言，如何改善上述缺失，使与既有的电脑界面可为相容，以达更佳的使用方便性是值得关切的课题。

发明内容

因此本发明的目的在于揭露出一新的技术，乃是将 USB 界面的储存卡，如智慧棒(1ritelligent Stick)，加入运算资料的控制，以满足并增加资料的安全性，达到资料保密(Security)的目的，而能应用于传统智慧卡的市场且又满足低系统成本及 USB 的泛用型界面的特性，且体积甚小而便于收纳于及使用。

一为实现上述目的，本发明提供的一种对资料加密保护的 USB 界面资料处理卡，至少具有一 USB 界面讯号，提供作为资料传输的方式；并具一 USB 界面控制器及一储存器单元，该界面控制器是处理界面资料后写入于该储存器单元，或处理该储存器单元内的资料后传

输至界面上；同时具有一运算单元，其是提供上述 USB 界面控制器的运算能力，以提供资料加密保护的功能。

所述的对资料加密保护的 USB 界面资料处理卡，其中储存器单元是由至少一储存器所组成。

所述的对资料加密保护的 USB 界面资料处理卡，其中 USB 界面控制器与运算单元是整合于一半导体晶片。

所述的对资料加密保护的 USB 界面资料处理卡，其中 USB 界面控制器与储存器单元是整合于一半导体晶片。

所述的对资料加密保护的 USB 界面资料处理卡，其中进一步包括有一乱码产生器，以作为产生资料加密处理所需的参数。

所述的对资料加密保护的 USB 界面资料处理卡，其中运算单元是可提供 DES、TDES、RC2、RC4、RC5、RSA、DSA、SHA/SHA-1、MD2 或 MD5 等的演算能力。

所述的对资料加密保护的 USB 界面资料处理卡，其中储存器单元进一步区分成数个区段，其中包括有一保护区段，使用者无法在此区段内部进行对资料的读取，写入、删除、修改及格式化等的动作。

所述的对资料加密保护的 USB 界面资料处理卡，其中进一步利用适当的程序提供，可使特定的使用者对该保护区段内部进行对资料的读取、写入、删除、修改或格式化等的动作。

所述的对资料加密保护的 USB 界面资料处理卡，其中该资料处理卡是使用智慧棒的结构设计。

附图说明

图 1 是本发明装置的系统方块图；

图 2 是储存器单元分割示意图；

图 3 是本案软件层架构示意图；

图 4 是本案加密型智慧棒外观示意图。

具体实施方式

详细说明，请参考图 1，所示为系统的方块图，其中包括 101、

为一 USB 界面控制器，负责资料的传输，102 为一储存器单元，是作为储存数位资料的地区，其与 USB 界面控制器具有适当的电路连接，103 则为一运算处理器，其与 USB 界面控制器及储存器单元，亦具有适当的电路连接。当资料经由界面控制器后，经过运算处理器的处理，如 DES、TDES、RC2、RC4、RC5 等对称性演算法后，即可对资料作加密或解密的功能，最后再存入至储存器单元或传输至外部作业系统。

而为了增加其资料安全性等级也可再使用非对称性演算法作进一步加密，如 RSA、DSA、ECC 等的运算方式，以符合并可使用于 PKI 的安全认证系统的运用，而进一步增加资料加密后的安全性。为方便并提高安全性设计，可于系统内加入一乱码产生器 104，利用此一乱码产生器，即可随机产生上述运算加密时所需的参数(KEY)，如此则更进一步地加强了资料的安全性。

而为了满足图 1 所示的硬件操作，在软件的设计上，必须完成适当的应用程序界面(API，Application Program Intertace)，以提供系统发展，完成撰写发展安全保密性的操作作业业系统。

而除了硬件演算的能力外，本案的设计，也针对储存器单元进行区块的分割，使其成为数个区块，分别具有不同的特性，计有：一般使用区，只读防写区(Read 0nly)及保护区(Reserved)。一般使用区是提供使用者一般的资料储存与读取。而只读防写区则仅提供使用者读取资料，但不可写入，删除及修改资料，除非使用者通过一认证的程序管制，如输入通行密码(Password)。而保护区，则为一般使用者不可读取，写入，修改，及删除资料甚至亦无法对其进行格式化(Format)的动作，此部份的资料，是只保留给特定的系统服务，通过上述的应用程序界面(API)而从远端进行对保留区资料存取的控制，如此更能增加本案 USB 储存卡的安全等级。此区块分割的方式是一般智慧卡所没有的硬件特性。

请参考图 2，所示即为一储存器单元分割示意图，其中 200 为储存器单元，201 为一般使用区，202 为只读防写区，203 为保护区。

请再参考图 3，图 3 所示为本案的软件层架构，其中 301 实体层，

在硬件的设计上，使用了一 US B 储存卡的智慧棒结构，302 驱动层，负责协呼叫用户主机与实体层之间的资料交互操作和处理上层应用对本装置的访问请求，其中满足了微软的 PC / SC 的设计规范，而 303 用户界面层，其满足了的 PKCS#11 标准界面和 MS CryptoAPI 界面的作业规范，301 应用层，则为本案所完成的高阶应用程序界面(API)，利用此高阶应用程序界面，开发者可以针对已经熟悉的编程界面进行系统开发。

因此藉由图 1 的系统方块图，及图 3 的软件层架构的实施，即可完成一低成本而又轻薄短小的加密性 USB 界面储存装置，而进一步可使用如图 4 所示的智慧棒而加以商品化为加密而藉由本案的 USB 界面安全操作系统设计，使用者不需购置昂贵的智慧卡读卡装置(SmartCardReader)，大幅度减少成本，而又得以缩小卡片的大小而增加方便性，USB 界面的导入，更提高了随处可用的实用性。

因此，本案所揭示者，乃较佳实施例的一种，举凡局部的变更或修饰而源于本案的技术思想而为熟习该项技艺的人所易于推知者，俱不脱本案的专利权范畴。

说 明 书 附 图

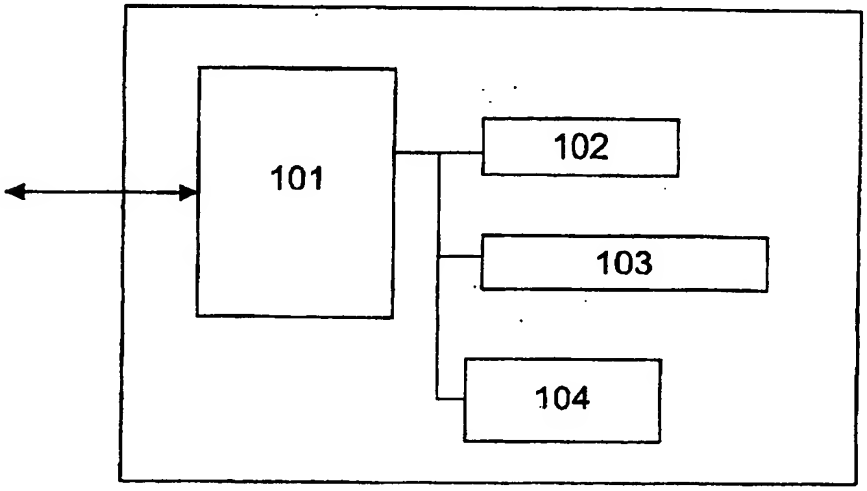

图 1

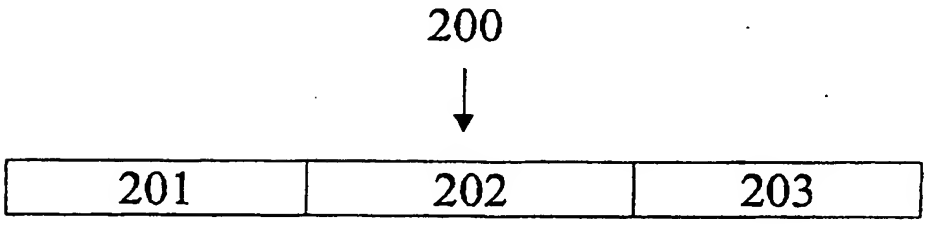

图 2

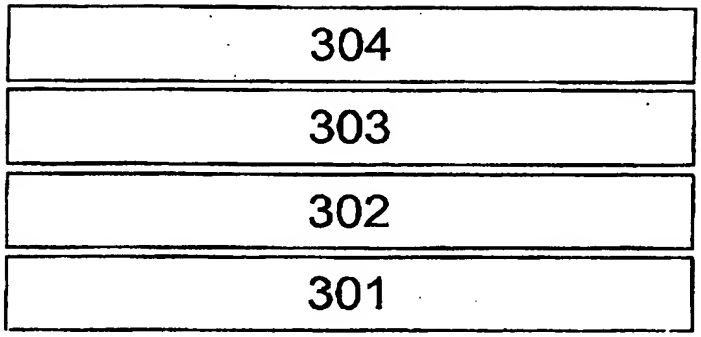

图 3

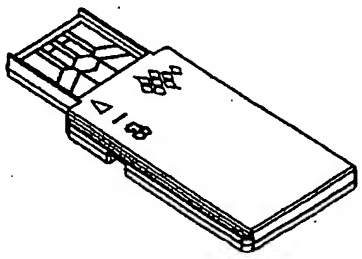

图 4